CISO'ENS GUIDE TIL PRINTSIKKERHET

2025

Canon

FORORD

For andre år på rad lanserer vi CISOens guide til printsikkerhet. For meg er dette en måte å vise at vi i Canon tar ansvar for å bevege printbransjen fremover, og å gi våre kunder verktøyene for å lykkes. Sikkerhet er et vanskelig tema å snakke om. Vi vet at det skjer mange flere datainnbrudd enn de som rapporteres om i media, og det skjønner jeg godt. For leverandøren er det tøft å måtte kommunisere sin rolle i en hendelse, og kunden vil kunne oppleve at det stilles spørsmål ved deres kompetanse.

Realiteten er at vi har en felles interesse i å stå sammen mot truslene – både leverandører, kunder, og individer. Feil vil alltid kunne oppstå, men om vi er gode til å dele kompetanse og erfaringer; vil det være færre feil som kan utnyttes, og flere vil kunne dra lærdom den gangen det går galt. Det er sunt samarbeid!

En viktig del av dette arbeidet må skje hos leverandørene. Kanskje særlig her i Norge, hvor vi er få folk i en global sammenheng, kan kompetanse være konsentrert hos få aktører. Jeg tror vi i Canon Norge er heldige og sitter på en betydelig del av sikkerhetskompetansen som finnes i vår bransje. Da har vi også et ansvar for å dele broderlig av den.

Denne guiden er vårt forsøk på å gjøre nettopp dette. Vi har samlet våre erfaringer gjennom de siste årene med et forhøyet sikkerhetsfokus, og strukturert de slik at det skal være lett å ta våre lærdommer i bruk i din organisasjon – enten du er kunde av oss eller ikke.

God fornøyelse!

Erik Mikalsen
Adm Dir
Canon Norge

FORMÅL MED GUIDEN

I denne guiden vil du finne en innføring i hvordan du sikrer ditt printmiljø, både på det praktiske og strategiske planet. Rådene er i størst mulig grad leverandørnøytrale og gir dermed et grunnlag for at IT-ledere i alle typer foretak effektivt kan forbedre sin print-sikkerhet. Canon mener printsikkerhet over tid har fått for lite fokus, relativt til informasjons-verdiene print-infrastrukturen behandler. Denne guiden er vårt bidrag til å hjelpe alle som benytter seg av printere i sin virksomhet.

Sammendrag:

Bakgrunn og nøkkelutfordringer:

I denne guiden fremheves printsikkerhet som et kritisk, men ofte oversett område innenfor informasjonssikkerhet i moderne organisasjoner. Printere, er i likhet med andre endepunkter som PC'er og servere, utsatt for ulike sikkerhetstrusler. Men, til forskjell fra disse, har printere en tendens til å bli neglisjert i organisasjoners sikkerhetsstrategier. Dette er bekymringsfullt, særlig gitt printeres oppgave knyttet til å behandle sensitive dokumenter. Vi peker i denne guiden på en mangel på kompetanse og bevissthet som hovedårsaker til denne neglisjeringen, og foreslår en systematisk tilnærming for å adressere disse utfordringene.

Strategisk tilnærming og tiltak:

For å håndtere utfordringene med printsikkerhet, foreslår vi en helhetlig tilnærming som inkluderer kartlegging av printere, identifisering av risikofaktorer, integrering av printere i eksisterende sikkerhets-prosesser, implementering av risikobaserte tiltak, og kontinuerlig oppdatering av kunnskap og praksis rundt printsikkerhet. Vi legger vekt på ressurseffektive tiltak og en pragmatisk risikostyringsprosess som hjørnesteiner for å lykkes med printsikkerhet. Videre understreker vi viktigheten av å forstå og vurdere personvernperspektivet, samt å håndtere sosial manipulering som et ledd i å fremme en helhetlig tilnærming til printsikkerhet.

Å se ting i sammenheng, og kontinuerlig forbedring:

Vi mener at kontinuerlig forbedring og oppdate-ring er sentralt for å opprettholde en robust print-sikkerhetsstrategi. Dette inkluderer aktiv dialog med leverandører for å utnytte nye sikkerhetsfunksjoner og -tjenester, samt å fremme en kultur for kontinuerlig læring og bevisstgjøring blant ansatte. Ved å innlemme printsikkerhet som en integrert del av organisasjonens overordnede sikkerhetsstrategi, kan virksomheter ikke bare redusere risikoen for datatap eller -lekkasje, men også forbedre etterlevelsen av personvernregelverk og informasjonssikkerhet generelt

Les også om informasjonssikkerhet på canon.no

INNHOLD

DEL 1: INNFØRING I PRINTSIKKERHET

Hva er printsikkerhet?

I Canon anser vi printsikkerhet som en form for endepunktssikring. Printere er som regel Linux-baserte datamaskiner med et stort antall grensesnitt og avhengigheter i organisasjonen.

Printere sikres ofte indirekte gjennom nettverks-sikkerhetstiltak, som brannmurregler og segmentering. Slike tiltak er viktige, men enhets-spesifikke tiltak burde, avhengig av brukerens konkrete situasjon og risikotoleranse, også iverksettes. Denne guiden vil ta for seg hvordan en sikrer printere direkte, hvilke betraktninger som burde gjøres rundt printerens grensesnitt, og hvordan printere kan passe inn i risikostyringen til brukerorganisasjonen.

Hvorfor prioritere printsikkerhet?

Som leverandør av printere, opplever vi i Canon ofte at printere uteblir, eller er i periferien av virksom-hetens tenkning rundt IT-sikkerhet. For eksempel kan PC'er, servere, og applikasjoner være omfattet av et modent styringssystem for informasjonssikkerhet, mens printere håndteres passivt, kanskje utelukkende merkantilt gjennom oppfølgning av driftsavtale, eller som en facilitytjeneste på linje med kaffemaskiner.

Denne modellen passer dårlig med virkeligheten: En printer skal kunne kommunisere med alle brukernes-PC'er og sentrale systemer i organisasjonen. De skal videre kunne håndtere både output og input av sensitive dokumenter, oppbe-vare filer som ligger på vent og noen ganger også ha en dobbeltrolle der printeren skal fungere innenfor og utenfor sikkersone. Store enheter står ofte uten direkte tilsyn, og de har ettersyn av eksternt personell, av ansatte og av intern IT. Dyptgående kompetanse på sikring av disse kan være mangelfull hos lokale IT-avdelinger.

Undersøkelser understøtter dette perspektivet: I følge Quocircas rapport, Print Security Landscape 2024, er det bare 13% av bedrifter som oppgir at de føler seg helt trygge på sikkerheten til print-infrastrukturen sin. Samtidig sier bare litt over halv-parten at de har gjort formelle sikkerhetsvurderinger knyttet til print. I Canon mener vi denne motsigelsen skyldes for lav kompetanse, noe som igjen fører til nedprioritering av printsikkerhet.

Printere er eksponert for samme type trusler som andre endepunkt datamaskiner, i tillegg til utfordrin-gene som følger av deres krav til fysisk tilgjengelighet og det faktum at deres output er fysiske dokumenter, ofte med sensitiv informasjon. Samtidig får enhetene lite oppmerksomhet fra IT-ansvarlige. Det betyr at printerne dine kan være lavthengende frukt for trusselaktører, men også at selv litt fokus på print-sikkerhet kan gi store sikkerhetsmessige gevinster, i forhold til investeringen!

Hva er viktige faktorer for å oppnå god printsikkerhet?

Fokus

Den avgjørende faktoren for å lykkes med print-sikkerhet, er at en må fokusere på det. Utfordringen er ofte at man har mange områder som skriker etter oppmerksomhet. Ettersom printeren «alltid» har eksistert og siden vedlikehold og konfigurasjon i veldig mange tilfeller er satt ut til en ekstern part, blir printeren lite synlig. Muligheten for å ha et høyt fokus på printersikkerhet over tid uten at ressurser blir omprioritert, er liten. Dermed må god printsikkerhet basere seg på ressurseffektive tiltak og eksisterende rutiner og prosesser. Målet er ikke at printsikkerhet skal bli et hovedfokus for foretaket, men at en skal ha et bevist forhold til sin tilnærming gjennom risikoforståelse.

Risikostyring

De siste årene har flere og flere, og også mindre bedrifter tatt i bruk styringssystem for informasjons-sikkerhet. Dette er en gledelig utvikling bla. fordi det tillater organisasjoner å angripe sikkerhetsrisiko på en strukturert og pragmatisk måte. Det er en sentral forutsetning for å gjøre riktige prioriteringer. I disse prosessene må også print-infrastrukturen innlemmes og forstås. Ved hjelp av en aktiv risikovurderings-prosess – innlemmet i en styringsprosess- kan en komme frem til riktige tiltak for print-infrastrukturen, og en blir mindre utsatt for vyer og trender når en skal finne riktige prioriteringer.

Helhetlighet

En vanlig utfordring når en skal integrere nye systemer, som print-infrastrukturen i sine prosesser, er at en ikke tar seg tid til å få nok kunnskap om hvordan dette påvirker det en jobber med. Ingenting eksisterer i et vakuum, ei heller printere. For å oppnå god printsikkerhet bør print-infrastrukturen kartlegges fra minst tre perspektiver:

Det tekniske infrastrukturperspektivet, med spørsmål som:

- Hvilke tekniske egenskaper har printeren?
- Hvor kan den nås fra på nettverket?
- I hvilken grad overholder den interne policyer med tanke på passordhåndtering, tillatte proto-koller og oppdateringer mv?

Dokumentperspektivet, med spørsmål som:

- Hva er de vanligste dokumentflytene?
- Hvor i prosessen ser vi brukerfeil som kan føre til at dokumenter kommer på avveie?
- Finnes det gode rutiner for riktig printerbruk og kan feilkilder reduseres gjennom tekniske tiltak?

Leverandørperspektivet, med spørsmål som:

- Tilbyr leverandøren de tjenestene og den oppfølg-ningen vi trenger for å utfylle vår egen kompe-tanse nå og i fremtiden
- Er leverandøren utsatt for sikkerhetspolitisk risiko?
- Har leverandøren selv solide og troverdige sikkerhetstiltak ved leveranse av produkt og tjenester, både før, under, og etter printerens levetid i din organisasjon?

Strategiske beslutninger og vurderinger – et utgangspunkt for å gjøre vurderinger knyttet til printsikkerhet

Det er vanskelig å gi en fullstendig oversikt over alle avgjørelser og prioriteringer en burde gjøre med tanke på å legge til rette for god printsikkerhet eller forbedre denne over tid. Under følger likevel noen vurderingsmomenter vi ønsker å trekke frem som et utgangspunkt for å oppnå godt fokus, levende risikostyring og en helhetlig tilnærming:

1. **Anerkjenn tradeoffs – enkel forvaltning og plug and play vs. sikkerhet:**
   Mens enkle passord eller standardpassord kan være enklere for administrasjon, kan de utgjøre en betydelig sikkerhetsrisiko. Sterke, unike passord kombinert med regelmessige passordendringer kan gi en mye høyere sikkerhetsstandard.

2. **Valg av Follow-me/ secure print-løsning:**
   Slike løsninger tilbyr viktige funksjoner som sikrer at dokumenter kun skrives ut når den autoriserte brukeren er fysisk til stede ved printeren. Dokumenter lagres og transporteres trygt hele veien fra endepunkt til endepunkt. Det reduserer risikoen for at sensitive dokumenter blir liggende på printerhyllen, tilgjengelige for uvedkommende- noe som er den vanligste kilden til tap av kontroll på informasjon ved bruk av printere.

3. **Ta hensyn til plassering:**
   Plasseringen av en printer kan ha en betydelig effekt på dens sikkerhet. Printere som er plassert i offentlige områder eller lett tilgjengelige for uvedkommende, er mer utsatt for uautorisert tilgang. Vær oppmerksom på hvilken informasjon som typisk blir skrevet ut på hver printer og vurder plassering basert på dette. En printer som ofte skriver ut konfidensiell informasjon, bør plasseres i et mer kontrollert og overvåket område.

4. **Hvor mye kompetanse?**
   Printere, som alt annet dere jobber med, krever spesifikk kompetanse for å bli forvaltet på en sikker måte. Sikre derfor at IT-avdelingen har riktig opplæring og kunnskap om printsikkerhet. Overvei også å jobbe med leverandører som tilbyr opplæring eller konsulenttjenester i dette området, avhengig av hva risikobildet deres tilsier.

5. **Arkitekturmessige vurderinger:**
   Tenk på hvordan printeren passer inn i organisasjonens IT-arkitektur. Dette inkluderer nettverksdesign, integrasjon med andre systemer hvordan printeren blir overvåket og aktivitet logget.

6. **Perimetersikring vs. Zero Trust:**
   Mens tradisjonell perimetersikring fokuserer på å beskytte grensene til nettverket, fokuserer Zero Trust på å ikke stole på noe innenfor eller utenfor nettverket og i stedet verifisere alt før det får tilgang. Vurder hvordan printeren kan beskyttes ved hjelp av Zero Trust-prinsipper, som for eksempel ved å kreve autentisering for alle utskriftsjobber eller ved å begrense tilgangen til printeren basert på brukerens rolle og behov.

7. **Sikkerhet gjennom bærekraftig bruk:**
   Bærekraft og miljø er viktige overveielser i moderne organisasjoner. Når du først tar aktivt grep for å konfigurere maskinparken – tenk på hvordan printerens funksjoner kan redusere avfall, for eksempel ved å oppmuntre til dobbeltsidig utskrift eller bruk av øko-modus. Vurder også å analysere bruksmønster for å finne ut hvor maskiner kan elimineres. Når du skal sikre en sikker avhending og sletting av kundeinformasjon, er dette også en god mulighet for å orientere deg om leverandørens rutiner for resirkulering og andre miljøorienterte livsløpstiltak.

Personvernperspektivet

Informasjonssikkerhet er et sentralt aspekt innenfor personopplysningsvern. Når en forbedrer printsikkerheten, forbedrer også organisasjonen personvernet. På samme måte vil mangelfull printsikkerhet naturlig føre med seg betydelig risiko for personvernet, ettersom sensitive dokumenter for eksempel i forbindelse med forskjellige former for saksbehandling, HR-prosesser, eller helsemessig behandling ofte ender opp innenfor printinfrastrukturen og til slutt bli skrevet ut. I tillegg oppbevarer printenheten og sikker print-løsningen selv opplysninger som alene eller sammenstilt med andre opplysninger krever personopplysningsvern. Et eksempel er printernes adressebøker som beskriver brukere registrert på enheten og tekniske forbindelser i organisasjonen, mens printlogger i utgangspunktets inneholder brukernavn, dokumentnavn og tidspunkt.

Det betyr at personvernperspektivet er viktig for å fastslå og vurdere risiko på en helhetlig måte. I motsatt tilfelle kan et enøyd perspektiv på teknisk sikring for eksempel være effektivt for å redusere risikoen for eksterne trusler, men forringe brukervennligheten til en slik grad at brukere tyr til skygge-IT, noe som kan skade personvernet langt mer en reduksjonen i sikkerhetsrisiko. God printsikkerhet er altså mer en god kontroll på teknisk konfigurasjon.

Som nevnt ovenfor er en levende risikoprosess en viktig forutsetning for å gjøre disse vurderingene. I slike forum kan interessenter med forskjellige kompetanser, herunder personvernansvarlige, møte for å sammen vurdere scenarier og tiltak. Forskjellige perspektiver vil føre til en bedre risikoforståelse.

Særlig når det gjelder printere, som har en betydelig slagside både fra et teknisk og bruker-perspektiv, er det avgjørende at personvernansvarlige blir involvert og satt i stand til å gjøre vurderinger. Det innebærer at teknisk personell må ha evne til å hjelpe personvernansvarlige å oversette en teknisk konfigurasjon til behandlingsprosesser. Printere er involvert i behandlingsprosesser som ikke avsluttes når printjobben er utført, men heller får sin start der. En fullstendig kartlegging av personvernrisiko ved bruk av printere har altså både et digitalt og et fysisk domene.

Nasjonal sikkerhetsmåned 2024: Våre digitale verdier

Årets tema valgt av norSIS er «Våre digitale verdier». Med digitale verdier mener norSIS alt av fotspor våre digitale liv skaper; som bilder, passord, dokumenter, og forretningsinformasjon. norSIS inviterer oss til å reflektere over verdien av alt det digitale innholdet som utgjør vårt digitale fotavtrykk, og hvilke risikoer som knytter seg opp mot disse.

Printeren er et nav for digitale verdier, både personlige og for organisasjoner. Det finnes et paradoks i dette: Vi ser at antallet sider som printes i vår brukermasse holder seg stabil, men befolkningen vokser og antallet digitale filer øker eksponensielt. Det betyr at en lavere andel av våre digitale verdier ender opp på papir, samtidig som det betyr at det som ender opp på papir er viktige dokumenter. : Det er kanskje bare de aller fineste feriebildene som printes, ikke de 2000 som ligger på telefonen. Mange avtaler signeres digitalt, men skal en printe ut en avtale r dette sannsynligvis en ekstra viktig avtale.

Det betyr at printere kan ses på som velegnede mål for datainnbrudd. For å avdekke om printeren kan være et attraktivt mål i din organisasjon, kan det være nyttig å kartlegge hva printerne i din bedrift benyttes til, sammen med hvor be fysisk befinner seg.

Nasjonal sikkerhetsmåned 2023: Sosial manipulering

Tema for 2023, valgt av NorSIS, var sosial manipulering. Sosial manipulering er en teknikk der trusselaktører utnytter menneskelige svakheter for å oppnå sine mål. Dette kan for eksempel være å lure noen til å gi fra seg passord, til å få tilgang til sikrede områder ved å utgi seg for å være en annen person, eller ved å legge press på individer.

Sosial manipulering kan finne sted i mange situasjoner, også i situasjoner der printere eller deres informasjonsverdier er mål. Printere, som tidligere nevnt, er ofte store maskiner som står for seg selv, som oppsøkes vel så ofte av tredjepartspersonell som av ansatte.

Dette gjør dem til et attraktivt mål for sosial manipulering. En trusselaktør kan for eksempel utgi seg for å være en tekniker som skal utføre vedlikehold på printeren og dermed få uinnskrenket tilgang til maskinen og potensielt sensitiv informasjon. En trusselaktør kan også få tilgang til printede dokumenter ved å late som de har glemt sin egen utskrift. Under har vi definert noen tiltak som kan bidra til sikring mot trusler som følge av sosial manipulering:

Bevissthet blant ansatte:

Det er viktig at alle ansatte er klar over risikoen for sosial manipulering og vet hvordan de skal håndtere mistenkelige forespørsler eller situasjoner. Dette kan oppnås gjennom regelmessig opplæring og simuleringer.
Autoritet: Sørg for at det er klart hvem som har autoritet til å utføre bestemte oppgaver på printeren. Dette kan for eksempel være vedlikehold, endring av innstillinger eller tilgang til lagrede dokumenter.

Sikring: Vurder å begrens tilgang til printere som er tiltenkt printing av sensitive dokumenter- f.eks. ved å plassere de bak dører med adgangskontroll.

Implementer smart overvåkning av printeraktivitet kan oppdage uvanlig eller mistenkelig oppførsel. Dette kan være store utskriftsjobber, utskrift av sensitive dokumenter utenfor vanlig arbeidstid, eller hyppige utskriftsjobber fra en bestemt bruker.

Kontroll på leverandører: Vurder om det må stilles krav til identifikasjon eller forhåndsinnmelding av serviceoppdrag slik at det er mulig for ansatte å avdekke forsøk på innbrudd.

DEL 2: HVORDAN MINDRE ORGANISASJONER KAN OPPNÅ BEDRE PRINTSIKKERHET

I denne seksjonen gir vi deg som er ansvarlig for IT-sikkerhet i en mellomstor eller mindre organisasjon noen korte tips som vil ta deg langt på vei til god printsikkerhet. Senere i denne guiden går vi mer i detalj på fremgangsmåte, men også tipsene her gir en god ledetråd for hvordan du kan gå frem.

Små og mellomstore organisasjoner har samme utfordringer når det gjelder å oppnå god printsikkerhet som større organisasjoner, men naturligvis mindre ressurser til å få på plass tiltak.

Kanskje tenker enkelte at de er for små til å være mål, men kriminelle aktørene som utfører brorparten av dataangrep er ute etter profitt, samme hvor den kommer fra. Derfor kan mindre organisasjoner være mer attraktive enn store – de har ikke nødvendigvis ressurser til å forhandle med trusselaktører om de har blitt utsatt for et datainnbrudd, eller kompetanse til å vedlikeholde en god backup av sine systemer. Dermed blir de tvunget til å betale mye for å unngå total driftsstans.

Dette bakteppet gir likevel ikke grunn til å bli motløs: Små organisasjoner har gode forutsetninger for å oppnå god kontroll og sikkerhet, bare de jobber smart. Samtidig unngår de glatt utfordringer knyttet til å skaffe oversikt og kontroll på en stor maskinpark fordelt på mange lokasjoner!

Enkle tiltak gir store gevinster

Det er som regel de enkleste tiltakene som har den største effekten. Enkle ting som dårlige passord, ikke oppdatert programvare, ubeskyttede dataoverføringer, eller mangel på fysisk kontroll står for en overveldende stor andel av uønskede hendelser. De viktigste tiltakene er altså de minst kompliserte.

Med en liten maskinpark er det overkommelig å holde kontroll på disse tingene, f.eks gjennom en halvårlig kontroll. Alle innstillingene nevnt over kan du selv kontrollere og sette på dine maskiner- oppskriften ligger i brukermanualen.

Still krav til printleverandøren din

Det du ikke klarer å gjøre selv, bør du ikke gi opp å få på plass. Ettersom produkter og tjenester blir mer komplekse, har det blitt til at leverandørene i økende grad tilbyr å ta på seg hele eller deler av driftsansvaret, herunder sikkerhet.

Slike tjenester er også tilgjengelige selv om du bare har en maskin. Det avgjørende blir da at du kritisk vurderer hva leverandøren kan tilby opp mot det sikkerhetsnivået du ønsker deg, og hvilken evne leverandøren har til å levere i tråd med avtalen.

Ikke neglisjer sikker print-løsning

Det vises i vår statistikk at andelen som benytter seg av en sikker print-løsning, synker ettersom antallet ansatte synker. Sikker print-løsninger er programvare som blant annet sikrer at bare individet som har sendt en fil til print, kan hente den ut på skriveren.

Dette kan for mange mindre organisasjoner virke overflødig, kanskje fordi bare de selv eller et begrenset antall personer de kjenner godt bruker printeren. Vårt råd er imidlertid å likevel undersøke om det finnes en egnet sikker-print løsning for deg. Årsaken til det er at sikker print-løsninger sikrer at dokumenter som behandles i løsningen alltid er kryptert fra ende til ende. På denne måten sikrer en seg godt mot at informasjon blir snappet av uvedkommende.

Praktiske skritt for å forbedre printsikkerheten

1

Kartlegg printinfrastrukturen:

Få oversikt over alle printere i organisasjonen, inkludert deres plassering, tilkobling og hvilke funksjoner de tilbyr. Dette gir grunnlag for å identifisere potensielle sårbarheter og prioriteringsområder.

2

Oppdater regelmessig:

Sørg for at alle printere har siste firmware og sikkerhetsoppdateringer. Sett opp rutiner for jevnlig sjekk og oppdatering.

3

Begrens tilgang:

Kontroller hvem som har fysisk og nettverkstilgang til printerne. Implementer tilgangskontroll både på bruker- og nettverksnivå. Steng funksjonalitet som ikke er i bruk.

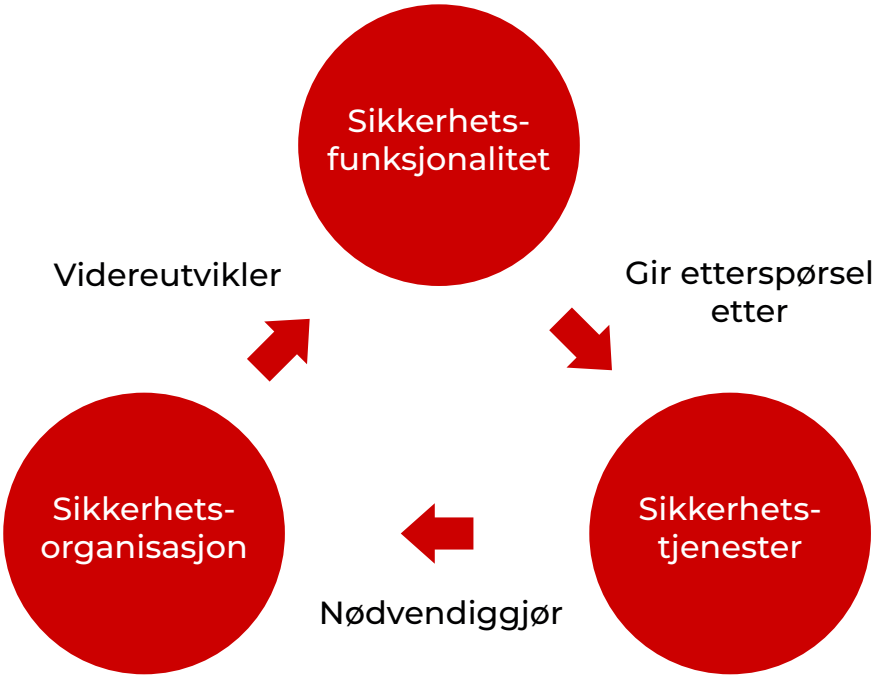
4

Øk bevisstheten:

Gjennomfør opplæring og informasjonskampanjer for å gjøre ansatte oppmerksomme på viktigheten

DEL 3: TIPS TIL SIKKERHETSKRAV I PRINTANBUD

Når organisasjoner skal anskaffe nye printløsninger eller tjenester, er det avgjørende å inkludere tydelige sikkerhetskrav i anbudsprosessen. Dette sikrer at de valgte løsningene møter dagens sikkerhetsutfordringer, men særlig tatt i betraktning den raske utviklingen, kombinert med lengre innkjøpssykluser, er det viktig at både leverandør og produkt i størst mulig grad er fremtidssikret.



I Canon opplever vi ofte at sikkerhetskravene som stilles, ser ut til å være hentet fra generiske lister over sikkerhetskrav beregnet f.eks for IoT-enheter eller «vanlige» endepunkt. Slike krav kan skape mye arbeid både for leverandører, og for kjøper, samtidig som de i begrenset grad er egnet til å avdekke forskjeller i produktene, eller i leverandørens kompetanse og kapasitet. Vi har derfor satt sammen en oversikt med forslag til krav og vurderingsområder vi mener kan være nyttige utgangspunkt for å formulere bedre krav knyttet til print og printtjenester. Kravene er fordelt i tre kategorier – leverandør, tjeneste, og produkt.

Leverandørkrav

Det er fornuftig å stille krav til ISO27001- sertifisering, da den på en effektiv måte sier noe om leverandørens modenhet hva gjelder IT-sikkerhet internt. Leverandøren burde spesifisere hva sertifiseringen dekker i organisasjonen. Leverandøren burde også bes spesifisere om det er særlige områder av sertifiseringens typiske omfang som ikke er dekket- f.eks ved å be leverandøren spesifisere om noen av kontrollene foreslått i ISO 27002 ikke er dekket. Et slikt krav kan «dekke mye terreng» og erstatte mange smalere krav, til fordel for både tilbyder og kjøper

Leverandøren bør forplikte seg til å følge personvernregelverket, og burde kunne forklare i sine egne ord hvordan den jobber med personvern, både lokalt og globalt. En demonstrert god forståelse for personvernregelverket vil også gi gode forutsetninger for avvikshåndtering og rapportering til myndigheter, dersom det skulle bli nødvendig.

Tjenestekrav

Det bør stilles krav til at sikkerhetstjenester beskrives utfyllende og konkret, slik at det er tydelig for kjøper hva tjenesten kan hjelpe med, og at det er mulig å sammenligne tjenestene som tilbys. Slike tjenester gjør kjøperen i bedre stand til å risikovurdere tjenesteleveransen og evt. planlegge kompenserende tiltak.

Det bør være krav om redegjørelse for hvordan tjenesten leveres- er det tredjeparter involvert? Hvordan behandles kundens opplysninger som en del av tjenesteleveransen? Slike spørsmål kan bidra avdekke leverandørkjederisiko.

Produktkrav

Produktet burde være framtidssikkret i den grad det er mulig. F.eks. burde enhetene støtte TPM2.0 for å holde tritt med implisitte eller eksplisitte minstekrav til krypteringsfunksjonalitet, særlig tatt i betraktning NIS2-direktivet.

Særlig for SaaS-løsninger bør det stilles krav om redegjørelse for personvernrisiko knyttet til overføring av data til tredjeland, og risiko knyttet til utilstrekkelig innebygget personvern. Er det f.eks. enkelt å slette brukerkontoer fra løsningen?

Leverandøren må kunne redegjøre for risiko i leverandørkjeden, også på et detaljnivå. Kjøperen må være i stand til å vurdere risiko både sikkerhetsmessig og fra et menneskerettighetsperspektiv f.eks. knyttet til produksjon av komponenter i land som NSM har flagget som høyrisiko, eller som Norge ikke har et sikkerhetssamarbeid med.

DEL 4: NIS2, OG HVORDAN NYE REGULERINGER PÅVIRKER KRAV TIL PRINTSIKKERHET

I takt med den økende digitaliseringen av samfunnet har cybersikkerhet blitt en kritisk faktor for alle organisasjoner. EU har, for å møte de stadig mer sofistikerte cybertruslene, vedtatt NIS2-direktivet (Network and Information Security Directive 2). Dette direktivet erstatter det opprinnelige NIS-direktivet fra 2016 og innfører strengere krav til sikkerhet for nettverk og informasjonssystemer.

Selv om Norge ikke er medlem av EU, vil NIS2 etter hvert innføres i Norge gjennom lov om digital sikkerhet. Loven er omfattende og det finnes susikkerhet rundt hvordan loven vil implementeres i Norge. Canon har registrert mange spørsmål om hvordan loven vil påvirke krav om sikkerhet på print. Under har vi delt våre vurderinger rundt vanlige spørsmål

Gjelder loven for min organisasjon?

Direktivet med fullstendig navn « gjelder en lang rekke Kritiske og Viktige organisasjoner i en rekke sektorer. Hovedkategorier er leverandører av nettverkstjenester, helsetjenester, tjenester innenfor offentlig forvaltning, og innenfor kraft og infrastruktur. Totalt sett vil mange enten være underlagt NIS2 direkte, eller jobbe med eller være leverandør til organisasjoner som er underlagt loven.

Det er også indikert minimumsgrenser for størrelse på organisasjonen, der organisasjoner som har mindre en 50 ansatte som små organisasjoner er fritatt. Organisasjoner med mellom 50 og 250 ansatte har lavere krav de må forholde seg til. Kritiske organisasjoner vil ikke være fritatt uavhengig av antallet ansatte.

I norsk målestokk er ikke en bedrift med mindre en 50 ansatte nødvendigvis liten, og siden NIS2 er et direktiv har Norge anledning til å tilpasse reglene til norske forhold. Det kan bety at mindre organisasjoner likevel vil være underlagt direktivet i Norge.

Et sentralt element av NIS2-direktivet er krav om at organisasjoner som er underlagt direktivet, skal vurdere risikoen i sin leverandørkjede, og å stille fornuftige sikkerhetskrav i anbudsprosesser. Dermed er det naturlig å forvente at organisasjoner som er underlagt NIS2-direktivet, vil stille krav til sine leverandører tilsvarende dem de selv er underlagt.

Ettersom direktivet ikke er innarbeidet i norsk lov, er det altså usikkert om du formelt sett vil være underlagt NIS2-direktivet, men det er likevel sannsynlig at NIS2 vil bidra til å etablere et forventet minstenivå av modenhet innenfor IT-sikkerhet i de fleste organisasjoner, ettersom nedslagsfeltet er bredt.

Hva handler NIS2 om?

NIS2 stiller ingen konkrete krav til sikkerhetsfunksjonalitet, men krav til fremgangsmåte og sikkerhetsorganisasjon, på 10 hovedområder[2].

- Risikovurderinger og sikkerhetspolicyer for informasjonssystemer.
- Policyer og prosedyrer for å evaluere effektiviteten av sikkerhetstiltak.
- Policyer og prosedyrer for bruk av kryptografi og, når det er relevant, kryptering.
- En plan for håndtering av sikkerhets-hendelser.
- Sikkerhet knyttet til anskaffelse, utvikling og drift av systemer. Dette innebærer policyer for håndtering og rapportering av sårbarheter.
- Opplæring i cybersikkerhet og praksis for grunnleggende datamaskinhygiene.
- Sikkerhetsprosedyrer for ansatte med tilgang til sensitiv eller viktig informasjon, inkludert policyer for datatilgang. Berørte organisasjoner må ha en oversikt over alle relevante eiendeler og sikre korrekt bruk og håndtering.
- En plan for håndtering av forretningsdrift under og etter en sikkerhetshendelse. Sikkerhetskopier må være oppdaterte, og det må finnes en plan for å sikre tilgang til IT-systemer og deres funksjoner under og etter en sikkerhetshendelse.
- Bruk av multifaktorautentisering, kontinuerlige autentiseringsløsninger, kryptering av tale, video og tekst, samt kryptert intern nødsituasjons-kommunikasjon når det er relevant.
- Sikkerhet rundt forsyningskjeder og forholdet mellom selskapet og direkte leverandører. Selskap må velge sikkerhets-tiltak som er tilpasset sårbarhetene hos hver leverandør, og deretter vurdere det overordnede sikkerhetsnivået for alle leverandører

Loven har altså ikke som mål å fortelle bedrifter hva de skal gjøre, men handler mer om å kreve at organisasjoner selv er i stand til å vurdere hva de skal gjøre. Det er naturligvis et omfattende arbeid, og en blir oppfordret til å se mot etablerte standarder og fremgangsmåter. F.eks. vil en ISO27001-sertifisering med kontroller implementert på disse forskjellige områdene, antageligvis bety at en også følger NIS2-direktivet.

2) NIS2 Requirements | 10 Minimum Measures to Address (nis2directive.eu)

Gjelder loven for print?

Loven gjelder som nevnt for organisasjoner, og handler om å opprettholde sikker drift/ produksjon. Om printere er en nødvendig del av din drift, eller om sikkerhetsbrudd på printere på annen måte kan påvirke driften negativt, er det et område kravene over gjelder for. Det betyr at printinfrastrukturen din må risikovurderes, og at det må implementere hensiktsmessige sikkerhetstiltak.

Hva kan jeg gjøre for å etterleve NIS2 på print?
Hva du må gjøre, vil variere avhengig av hva du kommer frem til i din risikovurderingsprosess. Det er likevel ikke noe ulempe å være sikrere enn en «egentlig» trenger å være. Vi i Canon anbefaler dermed å legge seg på den sikreste baselinen en kan, uten at det fører til ulempe på andre måter. Vår fremgangmsåte for herding finnes senere i denne guiden.

Hvordan kan printleverandører bidra til NIS2-etterlevelse?

De fleste leverandører av printere og print-tjenester kan tilby både rådgivning og betalte sikkerhetstjenester. I Canons tilfelle er vår herdingsstjeneste bygget på ekspertkompetanse og kartlagt mot beste sikkerhetspraksis. Å jobbe med leverandøren din kan dermed bli en «snarvei» for å oppnå riktig sikkerhetsnivå.

En forutsetning for å lene seg på leverandøren, er imidlertid at leverandøren må være tilstrekkelig sikker og i stand til å levere sikkerhetstjenester på en sikker måte. Særlig organisasjoner med svært høye krav til sikkerhet, burde dermed legge en innsats i å sikkerhetsvurdere leverandøren, før de eventuelt kjøper sikkerhetstjenester.

DEL 5: FEM SKRITT TIL BEDRE PRINTSIKKERHET

I denne seksjonen finner du en strukturert tilnærming til hvordan du kan bedre sikkerhetsnivået på- og i tilknytning til printerne dine. Oversikten er basert på typiske strukturerte tilnærminger til IT-sikkerhetsarbeid, men belyser printspesifikke utfordringer i tråd med Canons erfaringer. Vi har også koblet fremgangsmåten mot relevante tiltak fra NSMs grunnprinsipper, slik at det blir enklere å systematisere tiltakene mot et eksisterende styringssystem. Mange tiltak fra NSM kan være relevante for de tiltakene vi har definert, så oversikten er ikke nødvendigvis uttømmende.

1: Kartlegg printerne

TILTAK

- Kartlegg relevante egenskaper.
  Se eksempler under.
- Kartlegg arbeidsmønster og informasjonsflyt i din organisasjon.

ID, NSMS GRUNNPRINSIPPER

1.1.5: Kartlegg virksomhetens leveranser, informasjonssystemer og understøttende IKT-funksjoner.

1.1.6: Kartlegg informasjonsbehandling og dataflyt i virksomheten.

1.2.1: Etabler en prosess for å kartlegge enheter og programvare som er i bruk i virksomheten.

FORKLARING

For å oppnå forbedret printsikkerhet, må du først kartlegge egenskapene til printerne dine. Det kan variere hvilke egenskaper som er relevante å benytte ressurser for å kartlegge og å holde oppdatert. Vi anbefaler at minst egenskapene over er kartlagt og at denne oversikten holdes oppdatert. Dette arbeidet underbygger særlig senere arbeid med å etablere en sikker tilstand, eller sikkerhetsbaseline.

Relevante egenskaper er blant annet:

- Modelltype og merke
- Firmware-versjon
- Bruksoppgaver og fysisk plassering
- Hvem som har adgang til å gjøre konfigurasjonsendringer, og hvordan denne adgangen forvaltes.
- Åpne grensesnitt og funksjonen til disse.

2: Sett deg inn i printerspesifikke risikofaktorer i din organisasjon

TILTAK

- Gjør deg kjent med printerens særegenheter og hvilke risikoer de kan bringe med seg i ditt foretak. Eksempler under.
- Kartlegg dagens innretning mtp. Fysisk plassering, tilgangsstyring, og servicerutiner.

ID, NSMS GRUNNPRINSIPPER

1.1.5: Kartlegg virksomhetens leveranser, informasjonssystemer og understøttende IKT-funksjoner.

1.1.6: Kartlegg informasjonsbehandling og dataflyt i virksomheten.

1.2.1: Etabler en prosess for å kartlegge enheter og programvare som er i bruk i virksomheten.

FORKLARING

Når du har innsikt i din printer-infrastruktur, er det nødvendig å sette seg inn i hva som skiller printeren fra andre endepunkt i din infrastruktur. Disse særegenskapene vil ha innvirkning på hvilke risikoer som gjør seg gjeldende for din bruk av printere. Risikoene kan komme både av iboende egenskaper i printere, og hvordan du har valgt å integrere dem i infrastrukturen din for øvrig.

- **Printere står ofte uobservert over tid.** Dette øker risikoen for at det gjøres uautoriserte endringer på printeren uten at det oppdages.
- **Ofte en miks av ansatte og eksterne som benytter printeren (ansatte, kunder, potensielle ansatte og gjester, service-teknikere.** Øker risikoen for at uautorisert personell kan få tilgang til enheten, uten at det oppdages.
- **Ofte enheter både innenfor og utenfor sikker sone.** Dette øker risikoen for at en enhet som behandler sensitive dokumenter, ikke har passende sikkerhetskonfigurasjon
- **Printere har noen ganger «dobbeltrolle» som intern og ekstern enhet.** Øker risikoen for at eksterne kan få tilgang til dokumenter til intern bruk

3: Innlem printere i eksisterende sikkerhetsprosesser

TILTAK

- Benytt kompetansen du har tilegnet deg til å utføre en risikovurdering.
- Etabler risikobaserte tiltak
- Planlegg oppfølgning

ID, NSMs grunnprinsipper

3.1.1: Gjennomfør jevnlig sårbarhetskartlegging.

3.3.2: Etabler og vedlikehold kompetanse om normaltilstanden i virksomhetens informasjons-systemer.

4.1.2: Gjennomfør en analyse av virksomhetskritiske effekter.

FORKLARING

Uavhengig av hvordan og i hvilken grad du har formalisert risikostyringen i din organisasjon, er det viktig at risikonivå fastsettes slik at tiltak kan utarbeides der de trengs mest. Foregående skritt skal ha gjort deg i stand til dette på en god måte, ved at du har etablert en organisasjonsspesifikk kontekst for din bruk av printerparken din, og hvilke relevante egenskaper den har. På denne måten vil gjennomføring av både generelle og print-spesifikke tiltak kunne sees i sammenheng, noe som fører til mer effektfulle tiltak.

4: Implementer- alene eller med hjelp fra tjenesteleverandør

TILTAK

- Benytt risikovurderingen og tiltakslisten du har utarbeidet til å utføre målrettede tiltak.
- Gå i dialog med leverandør for å forstå mulighetsrom og fremgangsmåte for din maskinpark.
- Vurder om deler av leveransen kan og burde tjenesteutsettes.

ID, NSMS GRUNNPRINSIPPER

2.2.7: Etabler en robust og motstandsdyktig IKT-arkitektur.

ID 2.1.1: Integrer sikkerhet i virksomhetens prosess for anskaffelser.

ID 2.1.9: Ta ansvar for virksomhetens sikkerhet også ved tjenesteutsetting.

FORKLARING

Det er viktig å følge opp de tiltakene du har identifisert som nødvendige. Dersom du har lyktes i å innlemme printsikkerhet og din opparbeidede kunnskap om print og situasjonsbildet i dine eksisterende prosesser, vil imidlertid tiltak relatert til printsikkerhet enklere kunne identifiseres og prioriteres.

En viktig del av å lykkes med implementering, er å trekke på kompetansen til din leverandør- det er sjeldent et poeng å gjenoppfinne hjulet. I Dag vil de fleste leverandører også kunne tilby helt- eller delvis forvaltede tjenester som kan driftes etter virksomhetens krav og ønsker. Dette kan lette på byrden for de driftsansvarlige i organisasjonen, og tillate deg å satse på den kompetansen du trenger aller mest, men fordrer også at du som kunde har kompetanse til å følge opp leverandøren på en god måte, slik at dere kan spille hverandre gode, og slik at du kan evaluere både leverandøren og leveransen i seg selv.

5: Hold deg oppdatert- også på printere

TILTAK

- Strømlinjeform informasjonsinnsamling
- Planlegg kompetanseheving
- Ansvarliggjør og still krav til leverandør

ID, NSMs grunnprinsipper

3.1.2: Abonner på tjenester relatert til sårbarhets-etterretning.

3.1.3: Benytt automatisert og sentralisert verktøy for å håndtere kjente trusler (som skadevare).

2.1.10: Undersøk sikkerheten hos tjeneste-leverandør ved tjenesteutsetting.

FORKLARING

Når du har lyktes med å gjennomføre syklus med kartlegging, risikovurdering, og innføring av tiltak, er det også startskuddet for et kontinuerlig arbeid der printsikkerhet er en integrert del av sikker-hetsstyringen. Vellykket styring over tid krever en oppdatert kunnskap om printsikkerhet og en proaktiv tilnærming til nye trusler og beste praksis. F.eks. kan verktøyer for å varsle om relevante CVE'er benyttes for å trakke sårbarheter relatert til printere. I en litt bredere sammenheng finnes det flere arenaer for å holde seg oppdatert, som seminarer, kurs og nyhetsbrev.

Har du valgt å tjenesteutsette, er aktiv dialog med leverandører er viktig for å utnytte de nyeste sikker-hetsfunksjonene og -tjenestene. Samtidig er det viktig at du ansvarliggjør leverandøren og sikrer at de holder tritt med teknologisk og tjenestemessig utvikling både i leveransen, og som leverandør.

DEL 6: REFERANSER

Sikring av printenheter fra Canon:

Tiltak for å redusere risikoen for uautorisert tilgang på multifunksjonsprintere (Engelsk)

global.canon/en/support/security/pdf/mpf-office-production.pdf

Herdingsguide imageRUNNER Advance (Engelsk)

https://canon.a.bigcontent.io/v1/static/Canon_imageRUNNER_ADVANCE_Hardening_Guide_Brochure_EM_Digital_Final_DIGI

Sikkerhetswhitepaper- veiledning for herding av Canonprintere i tråd med NIST SP 800-171 og -172 (engelsk)

http://downloads.canon.com/nw/pdfs/solutions/NIST-Cybersecurity-Whitepaper.pdf

Canon brukermanualer på nett

https://oip.manual.canon/

Canons sikkerhetsiniativ og sikkerhetstjenester:

Sikre utskriftsløsninger fra Canon

https://www.canon.no/business/solutions/security/secure-printing/

Temaside sikkerhet i Canon[AK1]

https://www.canon.no/business/solutions/security/

Temaside personvern i Canon

https://www.canon.no/privacy/

KONTAKTINFORMASJON

Vi hjelper deg gjerne med spørsmål rundt sikkerhet.
Kontakt oss via vår nettside **canon.no.**

Våre øvrige kontaktopplysninger er

Besøksadresse:

Hallagerbakken 110

1256 OSLO

Postadresse:

P.O.Box 33, Holmlia N-1201 OSLO

Fakturaadresse:

Canon Norge AS

Postboks 1 Youngstorget 0028 Oslo Norway

Tlf. sentralbord:

+47 22 62 92 00